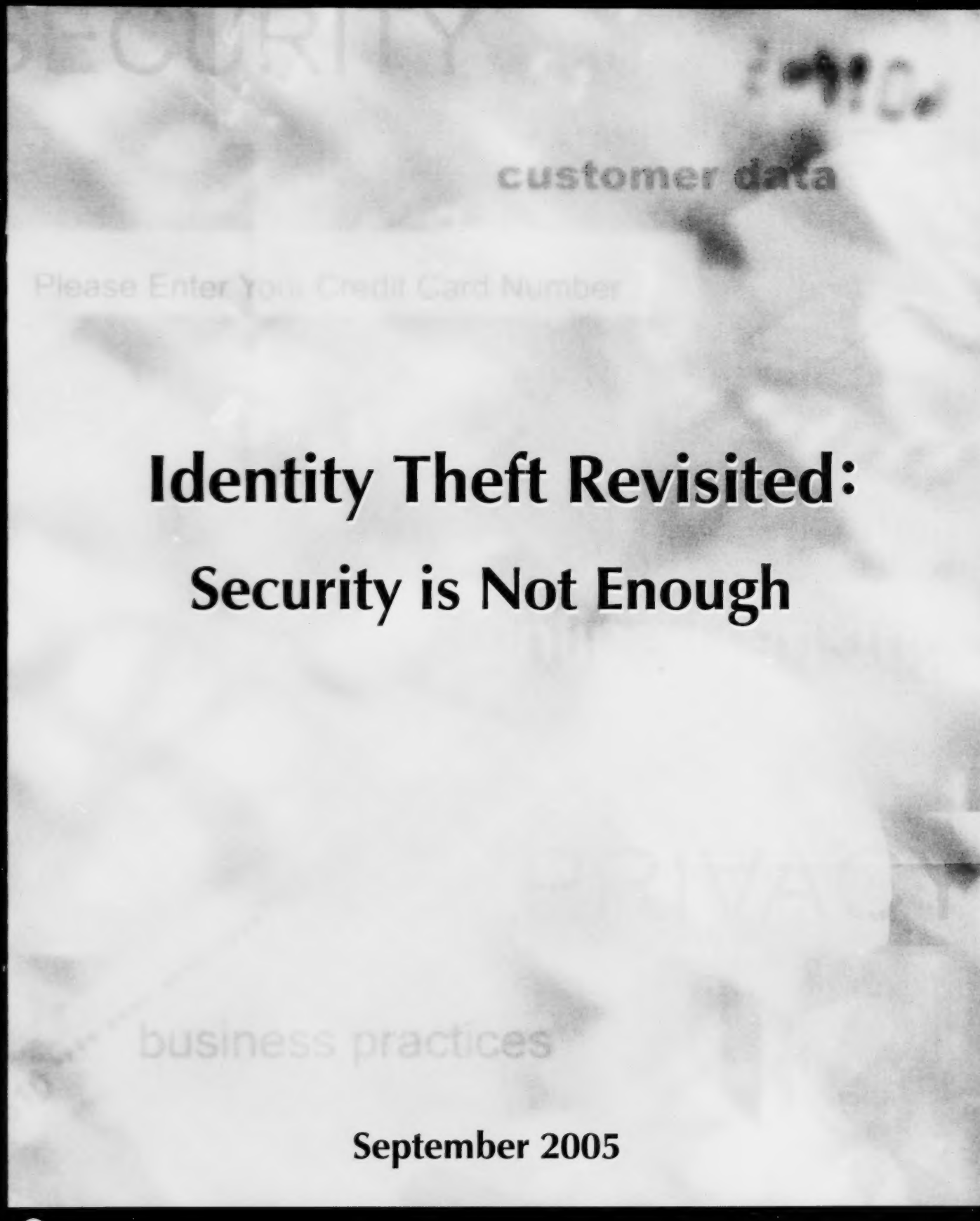

Identity Theft Revisited:

Security is Not Enough

September 2005

Information and Privacy Commissioner/Ontario

Ann Cavoukian, Ph.D.
Commissioner

Dr. Ann Cavoukian, the Information and Privacy Commissioner of Ontario, gratefully acknowledges the work of Fred Carter in preparing this document.

This publication is also available on the IPC website.

Information and Privacy Commissioner/Ontario

2 Bloor Street East
Suite 1400
Toronto, Ontario
M4W 1A8

416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Website: www.ipc.on.ca

Table of Contents

Executive Summary 1
The Problem of Identity Theft 2
Victims of ID Theft: The Consequences 4
Consumer Education and Awareness Efforts 4
Don't Blame the Victim 5
The Real Problem 5
The Incidence of Identity Theft: Recent Examples 6
Customer Data is Cheap but Valuable 8
Data Assets = Data Risks and Liabilities 10
Data Privacy = Good Data Security 13
Privacy is *Holistic*: Develop a Culture of Privacy 13
Fair Information Practices 14
Privacy is *Personal:* Consider the Individual's Interests 17
Privacy is *Comprehensive*: Privacy Enhances Security 20
Database Encryption 21
Severing or Encrypting Personal Identifiers 22
Data Aggregation, Perturbation and Anonymization 22
Data Item Masking 22
Identity Management/Access Controls 23
The Inside Job 24
Strong Authentication 24
Digital Rights Management (DRM) 25
Audit Trails / Electronic Tracking 25
Building a Culture of Privacy 26
Crisis Management 27
Consumer Self-Help Tips 28
Summary / Conclusions 29
End Notes 31
Select Bibliography 35
Relevant IPC Publications 35
External Sources Consulted 36

Executive Summary

Identity theft is becoming one of the most serious current-day threats to the public, impacting millions of innocent people every year. The problem is becoming so widespread that we must all become vigilant against the abuses of our personal information. If victimized, however, a considerable amount of time and money may need to be spent repairing the damage to our credit and reputation. The problem has permeated so deeply into our daily lives that it has given birth to a new type of commercial enterprise — "identity theft insurance services," which are now being marketed to a wide range of individuals seeking greater peace of mind.

The recent outbreak of high-profile security breaches within the last year has had the unintended benefit of exposing long term problems in the way that organizations have been managing their customers' data. Consequently, this has drawn the attention and critical scrutiny of the public, shareholders, and lawmakers. As a result, a wide range of legislative responses are being proposed based on the growing support for the mandatory notification of data security breaches, and for imposing a measure of liability on firms who mismanage their customers' data.

The prevalence of identity theft comes about as a result of many complex factors. When examined closely, however, we believe that the single largest cause of identity theft is the existence of poor information management practices on the part of organizations. There is a growing belief that organizations that collect, use and share personal information should bear greater responsibility for actions which negatively impact the public, and should take preventative measures to ensure the privacy of their customers' data. Placing this problem at the foot of consumers and expecting them to "protect themselves" is somewhat akin to expecting a child to safely navigate his way across a highway of speeding cars – he wouldn't stand a chance.

While we identify several steps that consumers can take to minimize becoming a victim of identify theft, the problem is largely out of their hands. We place the problem in the hands of organizations that collect massive amounts of personal information and leave it largely unencrypted and in clear view of both insiders and outsiders alike.

This is a critical time for businesses to take the opportunity to review and improve their information management and security practices. This is necessary, not simply to avoid negative publicity and litigation, but also to build enduring trust with customers, partners and stockholders. In an effort to do so, businesses should consider the fundamental insights that data privacy can offer to organizational security – privacy and security go hand-in-hand.

The Problem of Identity Theft

Identity theft is the Crime of the Information Age, *the* Crime of the 21st Century – an unfortunate by-product of the growth and velocity of personal data coursing through vast, interconnected e-commerce databases and networks.

Today, every aspect of our lives is somehow affected and mediated by a number of digital devices such as credit cards, ATMs, cell phones, and computers. Communications and data transfers are no longer limited to our place of work; they are now on our persons, in our cars, in our homes. As a result, through the use of various technologies, we invariably leave behind a lengthy trail of digital footprints.

From these digital tracks, others can reconstruct our digital histories, and with these data dossiers, map out who we are, what our interests and opinions are, who our friends are, where we have been, and predict where we will be going. With fewer face-to-face transactions and more remote automated decision-making, the potential to misuse these digital footprints can profoundly affect our lives by those who gather our data both openly, and indirectly.

Identity theft involves the use of a victim's personal information to impersonate them and illegally access their accounts, obtain credit and take out loans in the victim's name, obtain accommodation, or otherwise engage in transactions by masquerading as the victim. Identity theft also includes the acquisition or transfer of personal information as an instrument to commit these crimes in the future.

According to the U.S. General Accounting Office: "Identity theft or identity fraud generally involves 'stealing' another person's personal identifying information ... and then using that information to fraudulently establish credit, run up debt, or take over existing financial accounts."[1]

The IPC recognizes that there are significant differences between identity *theft* and identity *fraud*. True identity *theft* occurs when someone uses your personal information -- such as your Social Insurance Number or Social Security Number, birth date, mother's maiden name -- to impersonate you and apply for new credit accounts in your name. Identity *fraud* typically involves an unauthorized person using your credit card number from an existing account to make purchases. For the purposes of this paper, which focuses upon the information management practices of organizations that collect, use and share personal information, we will use 'identity theft' to refer to both.

Identity theft is the fastest growing white collar crime of the past decade, and the number one U.S. consumer complaint. A 2003 Federal Trade Commission survey estimated that nearly 10 million Americans were victims of some form of ID theft within the past year, triple the

number in 2001.[2] According to survey data released in July 2005 by Chubb Insurance, 20% –one in five—Americans has been a victim of identity theft or fraud.[3]

A recent survey conducted by Privacy and American Business ("P&AB") and Deloitte Touche found that 20% of respondents reported having been a victim of identity fraud or theft.[4] Dr. Alan Westin, one of the foremost privacy experts and publisher of Privacy & American Business, commented:Our survey shows that there does not seem to be a plateau as yet in the instances of identity theft, despite major attempts by business and government to stem the tide."[5]

Identity theft can and does take many forms. Personal information itself is sometimes used to obtain more detailed information on a targeted victim, and the methods are constantly changing. Computer viruses, "Trojan horses," "worms," keyloggers, and other malicious spyware, capable of harvesting personal information from the computers of unsuspecting owners and then "phoning home" with the data, have become an epidemic.[6] "Phishing" and "pharming" are the latest techniques, whereby scammers electronically masquerade as legitimate businesses, contact innocent accountholders, and request confidential data such as account numbers and passwords.[7] The techniques are constantly mutating: rather than posing as a bank or other online business, "spear phishers" send e-mail to employees at a company or government agency, making it appear that the e-mail comes from a powerful person within the organization. Once they trick employees into giving up passwords, they can install malicious software programs that ferret out additional sensitive information or secrets.[8]

Contrary to the popular myth that identity theft and fraud are carried out using high-tech methods by renegade computer geniuses, the fact remains that these crimes continue to depend on a steady and easily accessible supply of personally identifiable information (PII). Normally referred to as "tombstone data," information that is stolen by identity thieves includes a person's name, home address, account number, credit card information, social security/insurance number, driver's licence number, date of birth, mother's maiden name, passwords, and other personal details. Armed with enough personal data, identity thieves can take on many different "financial personas."

To put some perspective on just how little an identity thief needs to work with, research conducted at Carnegie-Mellon University determined that nearly 90% of the U.S. population could be uniquely identified through the use of only three pieces of information: a person's date-of-birth, sex, and postal code.[9]

Victims of ID Theft: The Consequences

In most cases, victims of identity theft have absolutely no idea they have become victims until it is usually too late. Out of the blue, the victim may find herself denied a purchase or a loan, denied a credit limit increase, or even denied an apartment rental – almost anything that involves a credit or background check. And then his or her life changes.

The effects of identity theft can be truly devastating. "Data rape" leaves deep scars on victims and consumes a significant amount of their time and effort. A great deal of time may be expended in persuading banks and credit bureaus to remove fraudulent accounts from their credit reports, or convincing creditors to stop reporting them as defaulters and deadbeats. Unpaid debts and collections can ruin a victim's credit score and creditworthiness, often leading to denials of mortgage and other credit. As the aggravation and frustration compound, the burden remains on the victim to write certified letters, keep detailed records and follow up with companies until the problem is resolved. Identity theft victims typically spend hundreds of hours, and dollars, in their efforts to clear their names.

Consumer Education and Awareness Efforts

Growing recognition of this epidemic has prompted consumer groups, government agencies, and businesses organizations to introduce consumer education and awareness efforts and to provide some measure of support for victims and others at risk. The advice typically takes two forms: one, a helpful collection of advice and tips on how to minimize the risk of becoming a victim; and two, advice and resources on what to do, and where to go, upon becoming a victim.

As consumers, we are told to be careful about disclosing and discarding our personal information, to buy shredders, avoid dumpster divers, select hard-to-guess passwords (and change them frequently), be careful of whom we do business with, read privacy policies, request copies of our credit reports each year, and generally, minimize the amount of personal information we divulge, intentionally or otherwise. (See Consumer Help Tips section below.)

The underlying theory behind helpful tips seems to be that if people become more vigilant, arming themselves with these remedial powers,[10] and take suitable precautionary steps, the risks and effects of identity theft can be significantly minimized. **We do not agree.**

Given the epidemic nature of the problem and the clear harm it bears upon victims, it shouldn't be too difficult to persuade people that it is in their own self-interest to be vigilant about their personal information, their identity, and their credit histories. But this approach

can be very misleading because it suggests that individuals can prevent the occurrence of this problem. For the most part, they cannot.

Don't Blame the Victim

Daniel Solove, a law professor at Georgetown University, has pointed out the problems that arise when individuals are expected to "take control" of their own digital dossiers, and exercise any rights available to them. Professor Solove points out that personal data is often collected unwittingly, without one's consent.[11] In the United States, a social security number (SSN) is a necessity of life in society and is vital for many activities from employment to renting an apartment. Refusal to give out one's SSN can result in much inconvenience and ultimately, the absence of services being provided. A credit report can be used in lieu of the SSN, but most people cannot even name the major credit reporting agencies, let alone know how to request copies of their credit reports. Even if someone did take this cautionary step, the risks are still out there and not necessarily minimized to any significance. "There is no way you can fully immunize yourself from identity theft because the information is, and always will be, out there."[12]

The Real Problem

While individuals may contribute to the growth of identity theft, their involvement in its prevention is, in our view, minimal. The incidence of identity theft has skyrocketed largely because of poor information management practices by organizations, especially relating to data storage and retention, coupled with the explosive collection of personally identifiable information (PII). Most PII collected is retained in clear text (thus in plain view), meaning that the data is not encrypted or encoded in any way, nor are the personal identifiers severed or separated from the data itself. Therein lie the biggest problems – poor information management practices, poor security, and poor data storage practices.[13]

Professor Solove adds: "The identity thief's ability to so easily access and use our personal data stems from an architecture that does not provide adequate security to our personal information and that does not afford us with a sufficient degree of participation in the collection, dissemination and use of that information."[14]

While certainly not new, the data security problem has only recently come into the spotlight. A comprehensive study of 4,000 U.S. businesses reported that more than half of them had suffered database security breaches in the past year.[15]

It is one thing to have someone pilfer through your mail, or your unshredded trash, looking for credit card records, receipts and statements to steal, but quite another when electronic databases are involved. The identity theft problem becomes considerably magnified by the widespread sharing, selling, trading, matching, accessing, copying, misuse and outright theft of large databases containing hundreds of thousands of detailed customer files. Why steal one identity when you can steal thousands of them, remotely, and without detection?

The Incidence of Identity Theft: Recent Examples

A recent string of major data security and privacy breaches resulting from loss, theft, insider abuse, and fraudulent access have thrust the issue of responsible personal information stewardship into the realm of the public, lawmakers, and the media.

Examples of recent security and privacy breaches include:

- June, 2005: CardSystems Solutions Inc, a firm that processes credit card transactions for MasterCard, Visa, American Express, and Discover, reported that hackers had stolen 40 million credit card numbers. CardSystems' CEO admitted that the company should not have been retaining consumer credit information that was compromised as a result of a hack. In violation of its service agreements with the credit associations, CardSystems had kept information on approximately 200,000 credit accounts for research purposes.[16]

- June, 2005: Citigroup reported that personal information on 3.9 million consumer lending customers of its Financial subsidiary was lost by UPS while in transit to a credit bureau. The data on the backup tapes were not encrypted.[17]

- May, 2005: Media giant Time Warner reported that it lost a container of computer tapes with company data including the names and Social Security numbers of 600,000 U.S. employees and their dependents. The backup tapes were not encrypted.[18]

- May, 2005: The U.S. Department of Justice reported the theft of a laptop computer containing travel account and credit information for as many as 80,000 Justice employees. The data on the laptop was protected by a password. [19]

- April, 2005: Online brokerage Ameritrade disclosed that it had lost a backup computer storage tape containing records for 200,000 of its customers. The tape was lost in transit. The data was stored in plain text format, unencrypted.

- April, 2005: Global Bank HBSC notified at least 180,000 people who used GM MasterCard credit cards to make purchases at Polo Ralph Lauren to replace their cards

because criminals may have obtained access to their credit card information. The issue was confirmed as a technology-related problem; Polo said that the credit card data in question was inappropriately stored in its point-of-sales software system. [20]

- April, 2005: DSW Shoe Warehouse reported that hackers had accessed data on 1.4 million credit card transactions and another 96,000 processed cheques in more than 100 stores over 25 states over a three month period starting in February 2004.[21]

- April, 2005: A California medical group notified 185,000 current and former patients that their financial and medical records may have been compromised following the theft of computers containing personal data. The theft occurred after the group copied plain text patient and financial information from its secure servers to two local PCs as part of a patient billing project and year-end audit.[22]

- April, 2005: A former employee of a Washington-area Blockbuster video store was indicted on charges of stealing customers' identities, and using them to buy more than $117,000 in trips, electronics, and other goods, including a Mercedes-Benz car.[23]

- March, 2005: Health care giant Kaiser Permanente notified 140 patients that a disgruntled former employee had posted confidential information about them on her Weblog. The health care giant learned of the breach indirectly in January, 2005, from the federal Office of Civil Rights.[24]

- March, 2005: Time Warner Inc. reported that computer tapes containing the names, SSNs, and other personal data of 600,000 current and former employees were lost during their delivery to a data-storage facility in March, 2005. "The information on the tapes is in a form that's not easily accessed." stated a company spokesperson. Time Warner later publicly adopted a recommendation and new policy that all backup tapes be encrypted.[25]

- March, 2005: LexisNexis reported a privacy breach in its database division, where hackers accessed more than 300,000 profiles, including SSNs and drivers licence numbers, more than 10 times the number originally reported. Poor computer access management practices –mainly stolen passwords– were blamed.[26]

- March, 2005: A thief had stolen a laptop with personal information on 100,000 University of California, Berkeley alumni, graduate students and past applicants. The information, including names, SSNs, and in some instances birth dates and addresses, was unencrypted, although the laptop was password-protected.[27]

- March, 2005: Boston college officials warned 120,000 alumni that their personal information may have been stolen when an intruder hacked into a school computer

containing the addresses and SSNs of college graduates. The computer system was not run by the school, but by an outside contractor, for looking up the names and phone numbers of graduates in order to solicit donations.[28]

- February, 2005: Bank of America confirmed it had lost backup tapes containing the personal information of 1.2 million federal employees. Some of those records contained information about senior U.S. congressional representatives. The data on the missing tapes were not encrypted.[29]

- November, 2004: Data broker ChoicePoint, having built a $1 billion annual business around their "core competency of verifying and authenticating individuals and their credentials," reported the unauthorized access of over 150,000 detailed records by scam artists over a period of one year. At least 700 known instances of identity theft resulted from this security breach. Poor access control and authentication procedures were blamed.[30]

- November, 2004: A major Canadian bank – the CIBC – repeatedly sent confidential customer files by fax to a U.S. junkyard over a period of several *years*, despite being advised on many occasions by the junkyard owner, of the incorrect fax number and the transmission of sensitive personal data.[31]

- Other security breaches have occurred due to small automated errors in the management of databases that can quickly become amplified into major security breaches, such as disclosure of drug users in the "To" (instead of Bcc) line of a marketing or communication email message. The "classic" example of this type of privacy breach involved pharmaceutical giant Eli Lilly, who in 2001 accidentally disclosed the e-mail addresses of 669 subscribers to its Prozac Reminder Service.[32]

Customer Data is Cheap but Valuable

The Perfect Privacy Storm: The recent security scandals have brought to the surface the extent of personal information being collected and used by businesses in an effort to "know their customers better," to predict their behaviour, and to make decisions about them.

Each time someone uses a cell phone, visits an internet site, turns on a cable TV service or swipes a credit, debit or loyalty card, they leave behind a digital trail. Companies track these trails for patterns and preferences, constructing personal profiles, which companies can then use to promote new products or target advertising to specified customers.

Digital footprints are valuable to advertisers and marketers, and will become even more so as tracking technologies continue to advance. Internet usage has become one of the most closely tracked activities in modern life, with dozens of companies specializing in selling software services that can track an individual customer as he or she moves around the Net, compiling a snapshot of their interests that can then be sold to advertisers. This information can then further be matched or compared with records about customers found elsewhere, to create new profiles and assessments of shopping habits.

Thanks to new information technologies and services, it is now more possible than ever for businesses to "know their customer." There is nothing wrong with this practice provided that the customer wants to be known, by having consented to the relationship. This may or may not happen. Companies routinely collect personal data from third parties, often in near real-time, to carry out background and reliability checks, to authenticate claims, and to develop a more comprehensive and intimate understanding of their customers. More and more of these types of "history" checks are being carried out in real-time to minimize business risks by assessing creditworthiness, health conditions, insurance claims history, purchases, lifestyle patterns, and so forth.

The emergence of these digital files has become the subject of intense debate about regulatory oversight. The amount of information being collected and traded in this new "infomediary" industry is estimated to be worth approximately $10 billion per annum.

In the wake of numerous high-profile customer-data breaches, companies that have not previously been subject to information security and privacy regulation should expect new regulations to mirror elements of existing laws. For example, following California's landmark *Database Breach Notification Security Act* ("SB1386"), which requires notice to be given to consumers of breaches in security of data held by a business or government agency, 18 other states have passed similar security breach notification laws in 2005, with numerous other security breach notification bills pending in other states (16 at last count). In addition, a number of breach notice bills have been introduced and are progressing at the federal level.

Other bills being contemplated at the state and federal levels in response to the security breaches and identity theft problems have provisions that seek to restrict certain organizations' ability to collect, use and share personal information, to strengthen prior notification and consent requirements, and to enhance the access and redress rights of individuals vis-à-vis those organizations.

From a privacy perspective, it is somewhat unnerving that these large databases are held by third parties that have no direct relationship with the people whose information they

possess, nor any obligation to provide data access or correction to those persons, yet this appears to be occurring with greater frequency.

As Information and Privacy Commissioner, I have been publicly calling upon the provincial government to introduce comprehensive private-sector privacy legislation. In light of the recent rash of security breaches, the poor information management practices those breaches have exposed, the epidemic of identity theft, and the eroding trust and confidence that consumers have in organizations to manage their personal information responsibly, I have renewed my call for private sector legislation that can serve the interests of both consumers and businesses alike by establishing an effective framework for transparency, accountability and trust.

For businesses that wish to start their planning, there's no need to wait for implementation instructions on how to secure consumer data – start now!

Data Assets = Data Risks and Liabilities

What is becoming abundantly clear is that when customer data begins to haemorrhage due to a company's negligence, it is customers who often suffer the most, in the form of financial losses, identity theft, poor credit ratings, etc. Innocent individuals end up paying the price for careless data security practices of organizations. That is to say, the negative externalities or costs of bad security practices are often borne not by the host organization, but rather by the customers themselves.

The lack of compelling risk and liability for businesses has led some to speculate that organizations lack strong economic incentives to invest in good data privacy and security practices.[37] If data security breaches need not be reported, and the cost of those breaches is largely borne by others (with little likelihood of causally connecting the breach to the resulting harm), then companies have few reasons to address the data privacy and security problem in a systemic way. Further, if the expense of dealing with privacy breaches is minimal compared to the overall bottom line, then there may be few incentives to address data privacy and security seriously; losses due to fraud and identity theft may be tolerated as the "cost of doing business."

To cite an example of the above, an investigative report was conducted to determine why Canadian banks still use ATM cards (with magnetic strip technology), which are increasingly becoming vulnerable to identity thieves. The alternative to magnetic stripe cards are "smart cards" which are implanted with a computer chip that uses encryption to protect the information, thus making them far more secure from identity theft. So, the question was asked: why are banks not embracing "smart card" technology? The primary reason would

appear to be cost. In 2003, bank experts estimated that it would cost Canada's banking industry $500-million to produce and implement the new "smart card" technology for the debit card system, while debit card fraud only costs $44-million in comparison."[38] Simply put, financially, it would appear that it is less costly for banks to assume the cost of identity theft than to implement a new, more secure system. Yet, there is growing recognition that it is unreasonable to have the burden and responsibility for vigilance placed upon the consumer when the vulnerabilities and risks are largely generated not by themselves, and at times, by unknown third parties.

Some laws and regulations do impose a "duty of care" on businesses to collect and manage sensitive personal information in special ways, such as to provide notice, obtain consent, and to provide access and correction rights. In the United States, the Health Insurance Portability and Accountability Act features data security requirements for electronic health data; Sarbanes-Oxley imposes responsibilities on publicly-traded companies to establish and maintain adequate internal controls over information systems, as well as an assessment of the effectiveness of those internal controls; Gramm-Leach-Bliley requires firms to ensure data privacy for consumers; the *Fair Credit Reporting Act* and the *Fair and Accurate Credit Transactions Acts* prescribe conditions for collecting and managing personal financial information, such as those contained in credit scores.

However, there are additional reasons for businesses to demonstrate greater care in guarding their customers' personal information against identity theft. Rena Mears, leader of the Privacy Services Group of Deloitte & Touche, made an astute observation:

> "There is a significant portion of the population that is becoming concerned about identity theft, and it is influencing their purchasing decisions. Companies need to understand this and leverage the internal control improvements they have made as a result of Sarbanes-Oxley to increase the integrity and security around the personal information they hold for their customers."[39]

As noted earlier, the recent security breaches have sparked an explosion of public concern about the current data management practices of businesses. The majority of the security breach notification bills introduced at the state and federal levels are modelled after California's SB1386, and require companies to notify individuals when their personal information has been lost or stolen. These new laws, when they come into force, will serve as a powerful stimulus to enhance the privacy rights of individuals. Had it not been for this one requirement to notify affected customers, the revelation of the ChoicePoint incident and other breaches that followed would most likely never have become a matter of public knowledge.

Beyond notification of security breaches, an inferno of other federal and state legislative activity has developed across the United States. As of May 2005, there were 39 bills pending

in 19 states proposing to regulate the use of personal information, with other bills responding to the growing privacy threats stemming from spyware, phishing, pharming, and other Internet-related threats. This movement has also fuelled other privacy firestorms. In addition to the above 39 bills, there were an additional 115 bills, pending in 40 states, that are seeking to protect and safeguard personal information when it comes to the data industry and overseas outsourcing.[40]

Transparency and accountability are fundamental privacy principles. Privacy laws typically seek to effect these principles in statute and regulation, usually going farther to prescribe rules and conditions for the collection, use, and disclosure of personal information by organizations, and to provide certain rights to individuals vis-à-vis those organizations that would collect and use their data. Privacy laws are usually based upon a widely recognized set of *Fair Information Practices* (FIPs), which we discuss later in this paper.

There is a fundamental change underway towards greater transparency and accountability by organizations and their practices of data management, assurances of security, and handling of information assets. What was once a competitive strategic marketing decision is becoming a regulatory baseline and market imperative. Poor or opaque information management practices, when exposed, and if serious, are provoking adverse consequences in the form of fines, lawsuits, public backlashes, damage to brand and reputation, lost business, growing penalties, and other containment costs.

Customers and lawmakers alike are demanding stronger remedies whenever wrongful, or negligent action involving their personal information takes place. According to a Privacy & American Business study, since 2000, 182 cases of consumer privacy litigation have been brought against 234 U.S. businesses, which have paid out more than $160 million in fines and penalties due to privacy and security litigation.[41]

Increasing awareness among the public and lawmakers is driving the growth of strong privacy management practices: "The need for proper privacy management is increasing, and U.S. businesses must implement more robust customer privacy policies now or face government intervention and severe customer backlash."[42] Organizations can mitigate business and legal risks by adopting a high standard of *proactive* data privacy and information management into their operations, and consistently demonstrating compliance with those standards.

One recent example of a proactive approach comes from Microsoft. In April 2005, Microsoft filed 117 "John Doe" lawsuits in the U.S. against suspected "phishers" hoping to catch some of the biggest offenders. The accused were allegedly trying to con people out of sensitive personal information, such as bank details, passwords, and social security details, by using fake MSN, Hotmail accounts and Web sites, and mass e-mail and pop-up ads. Because there is no specific anti-phishing legislation in the United States, the lawsuits were filed in the U.S.

District Court in Seattle under the *Lanham Act*. This is a federal trademark protection law that carries a maximum of US$1 million fine per violation.

However, this issue involves much more than mere compliance. If you treat privacy as a business issue, and think about it strategically, you will go much further to discovering a competitive advantage. "How can this legal problem create an opportunity to gain an advantage over one's competitor?" was the question asked in *Using the Law for Competitive Advantage* by George J. Siedel.[43] The answer lies, in part, in adopting comprehensive data privacy standards that can build enduring trust and loyalty.

One way to accomplish this is by applying the Fair Information Practices in a more comprehensive and rigorous manner than before. Professor Fred Cate, a leading U.S. academic and public commentator on information law, observed that, "The greatest failure of FIPPS [Fair Information Practice Principles] as applied today is the substitution of maximizing consumer choice for the original goal of protecting privacy while permitting data flows ... Compliance with data protection laws is increasingly focused on providing required notices in proper form and at the right time, rather than on ensuring that personal information is protected."[44]

What guidance can data privacy provide to security professionals tasked with securing large customer databases from SB1386 and similar breach notification laws? Read on.

Data Privacy = Good Data Security

Privacy is *Holistic*: Develop a Culture of Privacy

Like the best security practices, data privacy is comprehensive in its approach to protecting personal information. Although privacy always applies to individual data items ("any information about an identifiable individual"), it also takes into account a much broader environment. Data privacy asks principled questions at every step of the information lifecycle, from collection and use through to disclosure and disposal.

The Office of the Information and Privacy Commissioner of Ontario offers useful information tools and privacy management documents on its web site, www.ipc.on.ca, to help organizations improve their privacy practices and policies:

- map data assets, current flows and uses;
- carry out privacy gap, threat and risk analyses;

- carry out privacy impact and risk assessments;
- plan and execute a successful privacy program;
- build privacy into information and consumer technologies;
- adopt leading-edge best practices; and
- build strong consumer trust and loyalty.

Summary: "Put someone in charge, analyze vulnerabilities, make a plan, implement policies and procedures that address technology as well as business processes, train, monitor your service providers, and continually revolve back to evaluate and adjust your program on an ongoing basis."[45]

It is also important to remember that privacy is not the responsibility of *one* division, department, branch, manager or executive. All organizations, both public and private, need to implement a multi-purpose privacy team made up of members from across the entire spectrum of the organization. You need to develop a culture of privacy. Privacy is more than just an organizational contingency, it is a mindset — a way of thinking. Remember that while technology may look good, your customers don't interact with your technology. It will always be organizational behaviour that gains the trust of consumers.

Fair Information Practices

The comprehensive management and systemic approaches of privacy are evident in a basic set of principles called Fair Information Practices that form the foundation of all privacy laws and policies. In Canada, the 10 principles contained in the Canadian Standards Association *Model Code for the Protection of Personal Information*[46] are as follows:

- Accountability – *an organization is responsible for personal information under its control and shall designate someone who is accountable for the organization's compliance.*

Without basic accountability, there is little possibility of learning about security breaches, and no chance of taking appropriate remedial actions. A big part of the spam, phishing, pharming, and spyware problems, is the difficulty in establishing the source of the originator and holding them accountable.

"It's really only because of the California law that we now know," noted U.S. Senator D. Feinstein, sponsor of a federal data breach notification bill that would "require any agency or company that collects personal information to notify potential victims of identity theft when

a security breach is discovered; impose a fine of up to $50,000 per day for each day that a company fails to notify victims about unauthorised access to personal information."[47]

Tyler Hamilton, a renowned author and columnist on technology and the law, noted that "forcing companies to disclose privacy breaches right away gives victims a chance to fight back within a reasonable time."[48]

The presence of an accountable privacy officer provides an avenue for victims to seek correction to mistakes and errors and, in general, to seek redress.

- **Identifying Purposes** – *the purpose for which personal information is collected shall be identified by the organization at or before the time of collection.*

The practice of indiscriminately and excessively collecting personal information, on the theory that stockpiling the data is cheap and may yield new insights that would become valuable someday, will be increasingly called into question. Collecting more information than you need may, and in the future, will most likely expose your organization to greater liability and risk.

Strong privacy practices help to discipline the collection of personal information at the very start of the information lifecycle by requiring purposes to be specified in advance. If the purposes are clearly stated and made known to the individual at the time of the collection, that leads to a stronger basis for "choice" and "consent."

In addition, overly broad purposes such as "to improve customer service," or "to ensure security," will need to be justified in greater detail, particularly when a breach has occurred and questions of informed consent are raised.

- **Limiting Collection** – *the collection of personal information shall be limited to that which is necessary for the purposes identified, and collected by fair and lawful means.*

On the general theory that "more data is better," indiscriminate and excessive collection of personal information by organizations is a disturbing trend. But the more information that is collected, the greater the chances that some of it will be inaccurate and out of date. Depending on where the data came from and how it was acquired, there is a greater likelihood that it may have been collected by unlawful means – exposing firms to charges of deceptive business practices and breaches of contract. Further, collecting more information than is necessary for specified purposes may aggravate customers, and result in a loss of business.

- **Limiting Use, Disclosure, and Retention** – *Personal information shall not be used or disclosed for purposes other than those for which it was collected, and shall be retained only as long as necessary for the fulfillment of those purposes.*

Unauthorized disclosures and secondary uses of personal information stored in large databases is in many cases *the* central problem contributing to identity theft.

The solution to this problem is to minimize your risk and liability by limiting not just the collection, but the use, disclosure and retention of personal information in the care and custody of the host organization.

This can be relatively straightforward as in deciding not to collect personally identifiable information in the first place, or deciding to configure cash register receipts to mask or truncate portions of credit or debit card numbers on printouts. It might mean configuring internal networks and software clients to withhold or mask the transmission, or display of sensitive and unnecessary fields such as driver's licence numbers, to frontline customer relations staff.

If the purpose of collecting sensitive personal data from the customer is to carry out a credit check to assess their creditworthiness, then there may be little need to retain this data once the assessment has been made. The same concept applies to sensitive personal information collected from background checks and interviews of potential employees. Once the purpose is fulfilled and a decision has been made, the data should be purged from the system, after allowing for the possibility of challenge to the final decision. As long as sensitive personal information is kept past its expiry date, it will always represent a potential risk and liability.

Further, if the purpose of collecting sensitive personal data is to authenticate the customer or subscriber when that customer requests an account change, then any "common secret" should suffice instead of "open secrets" like mother's maiden name or SSN/SIN numbers. Wherever possible, authenticating a customer in person should not involve making a permanent photocopy or record of personal documents.

Retention and destruction schedules for customer information, regardless of storage format, should be an integral and verifiable part of any organization's data management system. Document destruction policies for physical and electronic media should be developed and distributed to all involved in the processing of customer data. The use of shredding for physical records and wiping or other permanent forms of destruction for electronic media should be strongly encouraged. Adherence with these policies should be closely monitored and verified. Preferably, the destruction schedule should be an automatic process to maximize the control of potential risks.[49]

Privacy should be viewed as a security improvement for all stakeholders. Data privacy builds customer trust; business privacy protects stockholder equity.

Privacy is *Personal:* Consider the Individual's Interests

While security and privacy share some important common qualities and features, security is *not* privacy. IT security professionals often make the mistake of believing that if customer data can be kept confidential and preserved from corruption, then privacy is guaranteed. [*See IPC "Privacy vs. Security: Common Misconceptions"*]

Security tends to look at information management practices from a top-down control perspective in an effort to protect company data, processes and systems from attackers. Privacy, on the other hand, protects the interests of the *individual*. Its central focus is to restrict the use of an individual's data to the purposes specified – the emphasis is on containment, not widespread use throughout the organization.

Information security typically refers to the controls deployed by an organization for the purposes of securely collecting, using, and holding all data. It applies to personal and non-personal data alike. Privacy protection, conversely, applies only to personally identifiable information and focuses on how the interests of the identifiable data subject — the person providing the information — are affected. Depending on the type of business, this may describe either a major portion of the data held by an organization, or only a small segment.

In another comparison, the Chief Security Officer (CSO) tries to optimize *organizational control*, often starting from a security perimeter mentality. The Chief Privacy Officer (CPO) on the other hand, seeks to maximize *personal control*, to ensure that the individual maintains control over their personal information and that authorized users do not misuse their data.

There is growing support for strengthening privacy practices that allow individuals to exercise greater control over the accuracy, completeness, timeliness, use, distribution and disposition of their own personal information. For example, U.S. identity theft victims can now obtain free copies of their credit reports (as Canadians have been able to do for years) and can request credit watches, or freezes, to be applied to their reports. As individuals are notified of security breaches involving their personal information, they will have the opportunity to access and view their entire record and any disclosures made for accuracy or lack thereof; they will also be able to request that changes, corrections, and deletions be made to their files.

The current legislative interest on behalf of the rights of the individual stems from fundamental data privacy practices expressed in the early 1970s by the U.S. Department of Health and Welfare, e.g.:

- provide data subjects with information about their data activities;
- obtain any form of consent for processing of personal data;
- permit opt-out of processing by data brokers;
- offer rights of access or correction; and
- assume liability for errors that harm individuals.

As expressed in these Fair Information Practices, an individual's interests are advanced by the following principles:

- Consent: *The knowledge and consent of the individual are required for the collection, use or disclosure of personal information, except when inappropriate.*

Most data privacy laws revolve around the concept of individual consent. This principle brings the individual directly into the picture by vesting him or her with certain participatory rights in the information and how it is managed.

Consent can take a wide variety of forms depending on the circumstances but in general, and as a best practice, consent should be fully *informed* and *explicit*. It will increasingly be unacceptable for organizations to ask people to consent to something that they know nothing about or understand.

In many cases, the consent principle also imposes a duty upon organizations that collect personal information to record consent preferences and to ensure that these preferences are honoured, especially when sharing data with third parties.

An important aspect of consent is that it may be revoked or withdrawn by the individual. Consent that cannot be revoked typically has less validity. Withdrawn consent often imposes an obligation on an organization to ensure that other organizations with whom it has shared that data also honour the revocation.

Firms that do not have processes in place for recording consent and for honouring requests for withdrawal (i.e., take me off your mailing list), will have to face the consequences. Witness the recent decision of the Federal Privacy Commissioner regarding a major bank's practice not to do so.[49]

- **Accuracy**: *Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.*

It is a long-established principle that individuals are entitled to expect that decisions made about them will be based upon accurate information and that, moreover, they are entitled to know about and inspect any files held about them in order to verify accuracy and request corrections, if necessary.

By the same token, organizations are obliged to ensure the accuracy of the personal data they hold and use for decision-making purposes. Some do this by encouraging and making it easy for their customers to access and amend their own information, such as accessing their "profiles" and preferences. Other firms maintain accuracy by routinely discarding personal records upon a pre-set expiry date.

As the old saying goes, "Garbage in. Garbage out." Inaccurate or out-dated information can result in correspondingly bad decisions. And if those decisions are automated and materially impact the individual — such as their ability to obtain employment, a promotion, credit, insurance, reasonable accommodations, travel, etc.— then there may be a basis for a complaint and remedial action. A significant percentage of data compiled on all of us, held in dossiers, and sold to businesses and governments by infomediary brokers and data aggregators, is inaccurate.[51] In a recent study, the U.S. Public Interest Research Group found that one in four credit reports contained serious errors.[52]

- **Openness**: *An organization shall make readily available to individuals, specific information about its policies and practices relating to the management of personal information.*

Individuals (not to mention business partners and affiliates carrying out due diligence activities, as well as regulators and other oversight bodies), cannot evaluate the privacy and security claims of organizations to assess their trustworthiness without some degree of openness. Sunshine is the best disinfectant, especially where there is cause for concern.

- **Access**: *Upon request, an individual shall be informed of the existence, use and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.*

The principle of "no secret dossiers" has typically accompanied the individual's right to access, inspect and, where possible, request amendments, corrections, or annotations to any files held on him or her. Access to credit reports has become a well-established privacy right in Canada and the United States that also applies to files detailing medical records or

payments, residential or tenant history, cheque writing history, employment history, and insurance claims.

As more organizations compile ever-larger records on individuals, and as the negative implications and uses of those files become more evident, there is every reason to believe that the access principle will be expanded to more and more domains.[53]

When revelations of the Canadian Human Resources Development Agency's "Longitudinal Database" became known to the public, containing as many as 2000 data items on millions of individual Canadians, the agency received over 75,000 access requests in one month before dismantling the entire database.[54]

Firms are well-advised to have systems in place that allow them to respond to access requests in a timely manner.

- Challenging Compliance: *An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual, or individuals for the organization's compliance.*

When misunderstandings, disagreements, and disputes arise, it is best for all parties to have established escalation and mediation procedures in place. In Canada, Privacy Commissioners and the courts serve in many instances as the forums for investigating and resolving disputes.

From the perspective of the individual, the availability of avenues of redress that include the possibility of adverse decisions, negative publicity, restoration of damages, fines, and other binding consequences on the organization in question can serve to strengthen the negotiation and ensure that the individual's concerns are addressed as early as possible.

Privacy is *Comprehensive*: Privacy Enhances Security

- Safeguards: *Personal information shall be protected by security safeguards appropriate to the sensitivity of the information. Safeguards must be assured through reasonable physical, operational, and electronic means.*

Typically, privacy principles and laws do not provide much detail or guidance on security, leaving it up to organizations to decide what constitutes "appropriate" and "reasonable" security measures.

While the IT community has the necessary expertise to define what reasonable security looks like, IT professionals still face the greater challenge of how to persuade the rest of the

company to adhere to reasonable security standards. Many of the privacy-breach incidents that have appeared in the headlines this year demonstrate a failure of business practices, not a failure of information technology.

Many of the security breaches identified may have been avoided if simple physical safeguards had been in place and adhered to: computer databases that were physically lost or stolen in transit, hard drives physically removed from computers, laptops gone missing from sidewalks, taxicabs, hotel rooms. In many instances, physical access to the data or media is all that is needed for a privacy breach to take place.

Similarly, the growing recognition of the ability of insiders to quickly attach peripheral memory and storage devices to computers to effortlessly copy large volumes of sensitive data is being met by new techniques and technologies that physically prevent this from happening. It's harder to steal the data if your USB memory stick won't connect, or there is literally no place to insert a floppy.

While physical security measures are important, they must increasingly be supported in depth by organizational and technological reinforcements. Below is a sampling of proven technological means of safeguarding data from unauthorized access and use. While these methods may not entirely eliminate the problem, they will surely lead to a significant reduction.

Database Encryption

After limiting physical access, the single most important action is to secure data by encrypting it, not just in transit, but also in its place of storage. That way, when the hard drive or laptop is physically stolen, or when the data is copied, the personal information stored on it cannot be accessed, read or used. If the data is encrypted, the need to report it as lost or stolen and to notify the subjects also becomes less urgent.

While this may seem somewhat surprising, most databases, even the high-end sophisticated ones, continue to store data in clear text format (unencrypted), and even more surprising, those large data stores are routinely transferred, synchronized and backed up using unencrypted, insecure transmission methods and media.[55] So why should it come as a surprise that personal data is routinely stolen and identity theft is on the rise? Yet intelligent, cost-effective information technologies that automatically encrypt critical data wherever they are stored across an enterprise —in applications, databases or backup tapes— exist today and are widely available, such as I.B.M.'s new x9 mainframe[56] and solutions from Ingrian DataSecure.[57]

Severing or Encrypting Personal Identifiers

Another proven approach is to encrypt or replace certain sensitive database fields, or to otherwise sever the personal identifiers from the data record itself. This may be achieved through the use of a link or pointer to the personal identifiers as is often done in health care establishments with patient records, so that the data, in effect, becomes anonymized. When AOL's entire customer database was stolen in 2003, containing millions of records, customers' real names and other personally identifiable information were not included because a "severance function" had been activated.[58] Standardized and hashed identifiers could be used to carry out privacy-enhanced data matches and checks without exposing any personally identifiable information. This is the core idea behind I.B.M.'s new suite of information management tools, called DB2 Anonymous Resolution.[59]

Data Aggregation, Perturbation and Anonymization

Other privacy approaches seek to manipulate the data in such a way that individually identifiable records cannot be retained. Aggregation, statistical perturbation, and other data anonymization techniques are important privacy-enhancing processes. Such techniques effectively strip away key identifiers and, with them, the ability of data recipients to be able to match and re-identify individual records. Such techniques allow the routine disclosure and active dissemination of data contained in forms, and for some purposes that are effective and statistically valid, but simply not identifiable to an individual.

Data Item Masking

The next best solution is to mask the sensitive elements of database records from being accessed, transmitted, displayed, printed or otherwise disclosed or modified. The personal information stays in the database record but is not accessible without proper authorization. For example, it may not be necessary for a customer service representative to see a customer's entire record. Nor should a customer's entire credit card number be printed on the sales receipt – four digits will suffice, with the remainder being masked. This is commonly referred to as "truncating" a number of the digits of one's credit card number.

Identity Management/Access Controls

Another solution is to set rigorous access controls on the database and its contents. Innovative new approaches are being tried in this area, notably by adding "metadata" to records and data items that can specify purposes, preferences and other conditions of use. Access controls, and other usage policies, can then be automatically enforced through the use of automated mechanisms that read and apply the metadata, such as:

- Role-based "need-to-know" use;
- Identity management and provisioning;
- Use of 2- and 3-factor authentication;
- Authorization.

It is common for organizations to fail in revoking access on a timely basis, so that former employees, including contractors and temporary employees, may still maintain their network credentials, (e.g., passwords), for a considerable amount of time after they have left the organization.

Effective access controls require good enterprise-wide identity management techniques. When an employee leaves an organization, their username, password, and other network access and authorization privileges should all be revoked at the very time of departure. There is no excuse for a delay in this action since it should be a simple and quick task to perform. The average company has more than 100 directories in which identity information is stored. I.B.M. estimates up to 60% of company access profiles are orphaned accounts (e.g., employees who have left the company or changed jobs) creating serious security gaps.

According to highly acclaimed U.S. security expert Bruce Schneier, "Identity management systems are critical for organization. But they're less about security and more about process efficiency. When someone moves around in an organization – gets hired, fired, promoted or goes on vacation – their access to resources changes. Identity management systems allow administrators to deal with their information accesses in one easy place."

It appears that Enterprise Identity Management Systems are now in great demand, with many products and systems available. For a comprehensive overview and authoritative study of identity management systems from a privacy point of view, see the comprehensive report from the EU Privacy and Identity Management in Europe (PRIME), entitled *Identity Management Systems (IMS): Identification and Comparison Study*.[60]

The Inside Job

Apart from human error and hacker threats, inside theft is a big problem. It is well known that insiders who access databases often have network authorization, knowledge of data access codes and a precise idea of the information they want to exploit.

Further, there are more unauthorized accesses to databases than corporations admit to their clients, stockholders or business partners. Gartner Group estimates that internal employees commit 70% of information intrusions, and more than 95% of intrusions that result in significant financial losses. A 2002 survey of 163 *Fortune* 1000 companies found that 70% of reported security breaches were linked to insiders.[61]

Another survey by the Computer Security Institute revealed that over half of all corporate databases had some kind of breach every year, with the average breach resulting in close to $4 million in losses.[63] And these are only the security breaches that are reported.

There is no magic bullet solution to the insider abuse of personal information. At some point, employees must be allowed a certain measure of trust and latitude to go about their jobs. However, a variety of new technologies and techniques are emerging that can help establish automatic and enforceable boundaries around data access, use and sharing, followed by the use of audit trails to detect fraudulent activity, after-the-fact.

Chief among these are technologies that impose strict network and database access controls. When supported by automated logging and audit trails, strong access controls can go some way to reducing abuse of data. Increasingly, organizations are "locking down" data from unauthorized copying by preventing peripheral memory devices, such as floppy disks and USB sticks, from connecting to computers and saving data. Hard drives that self-destruct or "phone home" when removed from their proper environment are examples of technologies that can deter insider theft.

Similarly, new technologies allow finer restrictions on staff ability to print or forward sensitive messages or personal data. Sophisticated network filtering devices are now being developed and deployed that can detect when sensitive information is being sent out through the network, for example, by email or email attachment, in a manner analogous to scanning incoming messages and attachments for viruses or inappropriate content.

Strong Authentication

Strong, reliable methods of authentication are necessary to ensure that only authorized individuals, both internal and external, can access and use the data. Many security breaches

are the result of poor access control procedures and technologies, by both staff and clients. Some typical authentication remedies are:

- Better password management and protection;
- Innovative use of new reminder phrases and password substitutes, such as "Passfaces;"[62]
- Increasing use of two- and even three-factor authentication, e.g., secure ID tokens, RFID-enabled "proximity" access cards, and biometrics; and
- Avoid using identification or passwords that are the default, easily guessed or accessible, e.g., social insurance/security number or mother's maiden name.

Equifax Canada, a large credit reporting agency, has deployed a system of authenticating the identities of individuals who request copies of their credit report by asking them a series of "out-of-wallet" questions derived from their credit histories, such that they and only they, would know the answers. So, for instance, you might be asked (among other questions) whether or not you have had a car loan, the amount of your monthly payments, and with whom the loan was held.[64]

Digital Rights Management (DRM)

DRM technologies also offer innovative approaches to managing and controlling sensitive information within a given work context or environment. These technologies can enforce fine-tuned controls over the use and disclosure of data by others, such as their ability to view, copy, print, or forward. DRMs can even auto-delete data or messages not required beyond a specified time period. In the event that data is leaked or exposed, DRM may also make it possible to track and trace the data itself.

Audit Trails / Electronic Tracking

A key issue to consider when purchasing a database security solution is making sure you have a secure electronic audit trail for tracking and reporting activity regarding confidential data, such as personal information.

Information systems and processes should be designed from the start to minimize the collection, use and disclosure of personal data.[65] Additional levels of checks and authorizations should also be employed to access higher levels of sensitive data. Default settings should always be set to "no access" unless authorized, rather than the opposite.

A record of all databases accessed should be kept to help detect, deter, and if necessary, prosecute misuse and abuse after the fact. Clear organizational policies should guide the use of these logs.

Network logging and monitoring can also serve as an important deterrent and enforcement tool. It should be carried out automatically, routinely, quietly, accurately, and without human intervention. For example, intrusion detection systems attempt to monitor database and network usage for anomalous behaviour, such as repeated log-in attempts or large file transfers.

Independent third party audit, attestation, and certification may also be desirable for some companies to credibly demonstrate compliance and earn greater trust, especially with downstream and upstream suppliers, and other business Web partners.

With regard to the privacy and security of customer data, all forward transfers and use of customer data with affiliates and partners should be assured by contract and other legal mechanisms. 80% of firms fail to conduct a regular assessment of their IT outsourcer's compliance with the host organization's information security requirements. Moreover, 70% fail to conduct a regular assessment of their IT outsourcer's compliance with the host organization's information security policies.[66]

Building a Culture of Privacy

The majority of the recent security breaches may not have taken place if there had been formal organizational mechanisms in place. For example, if fax numbers had been double-checked after complaints of misdirected faxes, or if client credentials had been verified prior to giving access to databases of personal information. Most important, there should always be a chain of command in place, consisting of individuals whose duties include dealing with security and privacy breaches.

Moreover, recklessness or simple carelessness of a single employee can undermine even the best technological countermeasures. Many security breaches are simply the result of human error, enabled by weak operational practices. For this reason, attackers will invariably focus on the weaknesses of people and processes —the weakest link.

A marginal number of companies have instituted comprehensive internal training and awareness programs for their employees to learn about privacy and security. New technologies also offer unparalleled opportunities to inform staff about company policies, their responsibilities, and how to meet privacy and security obligations.

Lack of Awareness: Conventional wisdom says that most individuals are simply not aware of the importance of security measures as they go about their daily routines. Heightening the awareness of all employees can go a long way.

Crisis Management

Although many organizations have a business continuity plan, surveys suggest that few have adequately been tested, and that most contingency plans never survive past the point of first contact with the reality of a privacy or security breach. A 2005 Ponemon Institute survey of corporate privacy practices found that only a third of companies use a formal process to monitor and report security breaches.[67]

In our view, all organizations should implement a Privacy Crisis Management Protocol immediately upon learning of the breach. The five steps of such a protocol consist of:

1) Containment: Identify the scope of the potential breach and take immediate steps to contain it: retrieve the hard copies of any personal information that has been disclosed; ensure that no copies of the personal information have been made or retained by the individual who was not authorized to receive the information and obtain the individual's contact information in the event that follow-up is required; and determine whether the breach would allow unauthorized access to any other personal information (e.g., an electronic information system) and take whatever steps are appropriate (e.g., change passwords and/or temporarily shut down a system).
2) Notification: Identify those individuals whose privacy was breached and, barring exceptional circumstances, notify those individuals accordingly: notify the individuals whose privacy was breached, by telephone or in writing; provide details of the extent of the breach and the specifics of the personal information at issue; and advise of the steps that have been taken to address the breach, both immediate and long-term.
3) Communication: Ensure appropriate staff within your organization are immediately notified of the breach; advise the Privacy Commissioner and other relevant oversight agencies of the breach and work together constructively with their staff.
4) Investigation: Conduct an internal investigation into the matter, linked to any external investigation. The objectives of the investigation are to: 1) ensure the immediate requirements of containment and notification have been addressed; 2) examine the circumstances surrounding the breach and determine what caused it; and 3) review the adequacy of existing policies and procedures to protect personal information.
5) Improving Practices: Address the situation on a systematic basis. In some cases, program-wide or institution-wide procedures may warrant review; in other situations, compensatory action or other forms of restitution for affected individuals may be warranted.

Consumer Self-Help Tips

While we have stated that consumers are not responsible for the large-scale occurrences of identity theft emanating from poor data management practices, there are nonetheless steps that can be taken to attempt to minimize the risk of becoming a victim of identity theft:

1. Minimize the amount of personal information you give out, especially online;
2. Do not give out your SSN/SIN, unless absolutely necessary; never disclose it online; never use it as a password;
3. Keep items containing personal information, such as your birth certificate, passport, citizenship card, etc., in a safe place;
4. Guard your mail from theft; add a lock to your mailbox;
5. Pay attention to your billing cycles; carefully review bills and statements on a regular basis; monitor your account balances and activity frequently;
6. Obtain and review your full credit report every year; mark the date in your calendar as a reminder;
7. Notify creditors immediately if your cards are lost or stolen;
8. Obtain a separate credit card dedicated to the exclusive use of your online purchases (with the lowest credit limit possible);
9. Shred all personal records and financial statements instead of just throwing them into the wastebasket;
10. Beware of dumpster divers: ask businesses that you deal with (like car rental agencies) to shred your application forms upon completion of their use;
11. Ask companies who print your entire credit card number on the sales receipt to consider truncating the number (so it doesn't appear in its entirety); and
12. Be very wary of responding directly online to any e-mail request for personal information sent by online service providers (phishing), or an alleged superior within your organization (spear-phishing). Instead, contact the institution or sender through another communication channel – call them by phone, using a pre-existing number.

If you have already become a victim:

1. Immediately report the crime to the police; keep a copy of the occurrence report;
2. Armed with the police occurrence report, advise all businesses with whom you have a relationship of the possible loss, theft, or misuse of your identity. Ask for stronger security measures — have a fraud alert placed on your accounts; start with the credit bureaus;
3. Cancel all your cards and accounts, and open new ones;
4. Document all the steps you have taken and your expenses to clear your name and re-establish your credit;
5. Have your credit reports annotated or possibly "frozen;"
6. Contact the Post Office if you suspect that someone is diverting your mail – beware of false change of address forms; and
7. Consider telling your employer, as an added precaution.

Summary / Conclusions

Privacy is Good for Business: A growing body of evidence indicates that organizations that adopt open and effective information management practices, which respect their customers' personal information, are benefiting in many ways.

The outbreak of recent high-profile data security breaches in 2005 has had the unintended benefit of exposing long-term problems in the way that organizations have been managing sensitive customer data. Consequently, this has drawn the attention and critical scrutiny of the public, shareholders, and lawmakers. In response, a wide range of legislative responses are being proposed based on growing support for the early notification of data security breaches, and for imposing some measure of liability on firms who mismanage customer data.

It is becoming recognized that the single largest cause of identity theft derives from poor information management practices. There is a growing belief that organizations that collect, use and share personal information should bear greater responsibility for their actions, especially in the case of negligence that negatively impacts consumers and the public. Preventative measures must be taken at the outset to ensure that customer data is strongly protected.

This is a critical time for businesses —to take the opportunity to review and improve their information management policies and practices. This is clearly necessary not only to avoid negative publicity and litigation, but also to build enduring trust with customers, partners and stockholders. Towards this end, businesses should consider the fundamental insights that data privacy can offer to organizational security, namely:

1. **Data Privacy is Comprehensive** – it applies not only to the data itself but to the entire environment in which that data is collected and used;
2. **Data Privacy is Personal** – the interests of the data subject must be considered and built into information systems and controls; and
3. **Data Privacy Enhances Security** – by minimizing collection, use, disclosure and retention of sensitive personal data, privacy-enhancing technologies can contribute to stronger data security.

In summary, a proactive approach to data privacy and security will position an organization as a leader, differentiate it from the rest of the pack, and pay handsome dividends in terms of reduced costs associated with crisis management and damage control. Most important, it will lead to improved customer trust, goodwill, and loyalty. Too many businesses avoid taking an "outlier" approach to data privacy and security: the tendency is to keep one's head down, stay in the middle of the pack, and try not to get too far in front (or behind) the others, for fear of being singled out for attention. We think you should do the opposite.

Over time, this will prove to be a poor business strategy, as privacy and security incidents will invariably occur. However, the most proactive, open and accountable firms will suffer the least from the fallout. A proactive approach will provide an important head start on the coming wave of privacy legislative and regulatory measures being proposed and adopted across the United States and in Canada. Our advice — get in front of the crowd, develop strong information management practices, encrypt personal information holdings, and reap the benefits.

End Notes

1 U.S. General Accounting Office, *Identity Theft: Greater Awareness and Use of Existing Data Are Needed.* Washington, DC., June 2002, Document #GAO-02-766, p.23: www.consumer.gov/idtheft/reports/gao-d02766.pdf. The U.S. Federal Trade Commission has adopted a similar definition, i.e.: "Identity theft occurs when someone uses your personal information such as your name, Social Security number, credit card number or other identifying information, without your permission to commit fraud or other crimes." See www.consumer.gov/idtheft/.

2 Federal Trade Commission, *National and State Trends in Fraud & Identity Theft, January–December 2004*, February 1, 2005, www.consumer.gov/sentinel/pubs/Top10Fraud2004.pdf.

3 Chubb Insurance, news release: "One in Five Americans Has Been a Victim of Identity Fraud", July 7, 2005 http://www.chubb.com/corporate/chubb3875.html See also Ipsos-Reid, "Concern About Identity Theft Growing in Canada" survey results at: www.ipsos-na.com/news/pressrelease.cfm?id=2582.

4 Privacy & American Business and Deloitte & Touche LLP, *New Survey Reports An Increase in ID Theft and Decrease in Consumer Confidence*, Survey results released June 29, 2005 available at: www.pandab.org/deloitteidsurveypr.html.

5 Ibid.

6 See, for example, Ingrid Marson, "Identity theft ring affects at least 50 banks" in ZDNet, August 08, 2005 For more information on spyware see www.cdt.org/privacy/spyware/ For an inventory of spyware bills and similar legislation, see www.benedelman.org/spyware/#legislation.

7 For more information see www.antiphishing.org.

8 Reuters, "Online Scammers Pose as Execs in 'Spear-Phishing' " reported in eweek.com, August 17, 2005 at www.eweek.com/article2/0,1895,1849431,00.asp See also http://en.wikipedia.org/wiki/Phishing.

9 L. Sweeney, "K-Anonymity: A Model for Protecting Privacy," *Int'l J. Uncertainty, Fuzziness, and Knowledge-Based Systems*, vol. 10, 2002, pp. 557–570.

10 Such as requirements for informed "affirmative" consent as well as data access and correction rights.

11 Solove, Daniel J., Identity Theft, Privacy, and the Architecture of Vulnerability, *Hastings Law Journal*, Vol. 54, p. 23, 1227, 2003, p. http://ssrn.com/abstract=416740.

12 Ibid, p. 23

13 The problem of identity theft is further exacerbated by widespread poor authentication practices of businesses that allow fraudsters to make purchases, open new accounts, and obtain credit, etc. "Pre-approved credit card offers" are perhaps the most well-known example. Some industries (debit-card, cell phone) write off the costs of bad accounts as an acceptable cost of doing business – see discussion in report of Consumer Measures Committee, Working Together to Prevent Identity Theft - A Discussion Paper (July 2005) esp. pp. 6-7.

14 Ibid, p. 24

15 Cf. CSI/FBI Computer Crime and Security Surveys, available at http://www.gocsi.com/.

16 See news coverage at: www.msnbc.msn.com/id/8260050/ and www.msnbc.msn.com/id/8286132/.

17 See news coverage at: http://money.cnn.com/2005/06/06/news/fortune500/security_citigroup/.

18 See news coverage at: http://money.cnn.com/2005/05/02/news/fortune500/security_timewarner/.

19 See news coverage at: www.washingtonpost.com/wp-dyn/content/article/2005/05/31/AR2005053101379.html.

20 See news coverage at: http://news.com.com/2061-10789_3-5672286.html?part=rss&tag=5672286&subj=news.

[21] See news coverage at: http://searchsecurity.techtarget.com/columnItem/0,294698,sid14_gci1081866,00.html and www.informationweek.com/story/showArticle.jhtml?articleID=161601930.

[22] See http://judiciary.senate.gov/testimony.cfm?id=1437&wit_id=729.

[23] See news coverage at: www.washingtonpost.com/wp-dyn/content/article/2005/04/25/AR2005042501411.html.

[24] See news coverage at: www.networkworld.com/news/2005/0316kaiseperma.html?nl.

[25] See news coverage at: www.boston.com/business/technology/articles/2005/05/03/snafu_puts_600000_at_security_risk/.

[26] See April 12 press release, *LexisNexis Concludes Review of Data Search Activity, Identifying Additional Instances of Illegal Data Access* available at: www.lexisnexis.com/about/releases/0789.asp.

[27] See testimony at http://judiciary.senate.gov/testimony.cfm?id=1437&wit_id=729

[28] See news coverage at: www.msnbc.msn.com/id/7221456/.

[29] See coverage at: www.theregister.co.uk/2005/06/07/citigroup_lost_tape/ and www.msnbc.msn.com/id/7032779/.

[30] For a thorough chronology, see EPIC's ChoicePoint web page at: www.epic.org/privacy/choicepoint/.

[31] See factual account by Privacy Commissioner of Canada, "CIBC's privacy practices failed in cases of misdirected faxes" report of April 18, 2005 at www.privcom.gc.ca/incidents/2005/050418_01_e.asp and addendum at: www.privcom.gc.ca/incidents/2005/050418_02_e.asp.

[32] See FTC report and settlement of April 18, 2003, "Eli Lilly Settles FTC Charges Concerning Security Breach" at www.ftc.gov/opa/2002/01/elililly.htm.

[33] See Robert O'Harrow, *No Place to Hide: Behind the Scenes of Our Emerging Surveillance Society* (Free Press, 2005) book website at: www.noplacetohide.net.

[34] 2005 Breach of Information Legislation (updated as of July 20, 2005), National Conference of State Legislatures, available at: www.ncsl.org/programs/lis/CIP/priv/breach.htm.

[35] Ibid. See also inventory of new Consumer Report Security Freeze Legislation at www.ncsl.org/programs/banking/SecurityFreeze_2005.htm.

[36] See, for example, Declan McCullagh, "Senate moves toward new data security rules," in CNet July 28, 2005 http://news.com.com/2102-7348_3-5808894.html?tag=st.util.print and "Data-Security Bill Advances In Senate," at www.wfmynews2.com/2wtk/consumernews_article.aspx?storyid=46600.

[37] See, for example, Ross Anderson, Why Information Security is Hard - An Economic Perspective, 2001, at www.ftp.cl.cam.ac.uk/ftp/users/rja14/econ.pdf and Jean Camp, *et alia*, www.infosecon.net.

[38] CTV News, W-Five, "Debit Card Fraud", January 8, 2005.

[39] Cited in Privacy & American Business and Deloitte & Touche LLP, *New Survey Reports An Increase in ID Theft and Decrease in Consumer Confidence*, June 29, 2005 at: www.pandab.org/deloitteidsurveypr.html.

[40] Briefing from Privacy & American Business, *Privacy Legislation in the States.*

[41] Briefing from Privacy & American Business, *Consumer Privacy Litigation.*

[42] Walter Janowski, Research Director, Gartner , 19 May 2003. See www.gartner.com/5_about/press_releases/pr19may2003a.jsp.

[43] *Using the Law for Competitive Advantage*, George J. Siedel.

[44] Cate, Fred H., "The Failure of Fair Information Practice Principles," forthcoming in *Consumer Protection in the Age of the 'Information Economy'*, a draft manuscript for a forthcoming book. Quoted with the author's permission.

[45] Stampley, Dave, *Three Ways to Prepare for the IT Impact of New Privacy Laws*, InformationWeek, May 2, 2005: www.informationweek.com/story/showArticle.jhtml?articleID=161600945.

[46] See www.csa.ca/standards/privacy/Default.asp?language=english .

[47] Senate Takes up Data Security Law, Internet News, June 16, 2005 at www.internetnews.com/security/article.php/3513201 and April12, 2005 at www.internetnews.com/bus-news/article.php/3497161. See also http://feinstein.senate.gov/05_releases.html.

[48] Tyler Hamilton, "Web, databases feed identity theft", The Toronto Star, Dec. 9, 2002 at www.tecrime.com/llartl16.htm.

[49] Ann Cavoukian, Ph.D., "Privacy: Strong Information Practices are a Must - From Collection to Destruction.", NAID News, September 15, 2005.

[50] Privacy Commissioner of Canada, PIPEDA Case Summary #308: Opting-out of marketing inserts in account statement at www.privcom.gc.ca/cf-dc/2005/308_20050407_e.asp. Coverage at www.michaelgeist.ca/index.php?option=content&task=view&id=907.

[51] See, for example, the May 2005 survey at www.privacyactivism.org/docs/DataAggregatorsStudy.pdf.

[52] http://uspirg.org/uspirgnewsroom.asp?id2=13650&id3=USPIRGnewsroom&.

[53] See FTC report on online access available at www.ftc.gov/acoas/.

[54] The number of Privacy Act requests received by HRDC as a result of the May 2000 news story jumped from 8,443 in Fiscal Year 2000 (which ended on April 30, 2000) to 75,669 in Fiscal Year 2001 (Treasury Board Secretariat 2000, InfoSource Bulletin Number 23. Ottawa: November 2000 p. 14; Treasury Board Secretariat, Ottawa: August 2001, InfoSource Bulletin Number 24: p. 13).

[55] Only 7% of businesses encrypt all backup tapes, and even fewer encrypt data at the application or database layer, according to a March 2005 research report by Jon Oltsik and John McKnight at Enterprise Strategy Group, *Information at Risk: The State of Backup Encryption* available at www.enterprisestrategygroup.com/_documents/Report/Attachment2ID393.pdf.

Cited May 4 2005 in "After Data Losses Like Time Warner's, Companies Need To Rethink Tape-Storage Security," *InformationWeek* at www.informationweek.com/shared/printableArticle.jhtml?articleID=162101437.

[56] See "I.B.M. Introduces New Line of Mainframe Computers", reported in *The New York Times*, July 17, 2005 at www.nytimes.com/2005/07/27/technology/26cnd-ibm.html?

[57] Ingrian DataSecure Solutions at www.ingrian.com/products/ and www.ingrian.com/news/pr050627.html.

[58] However, 92 million AOL usernames and email addresses *were* stolen and used illegally to send billions of spam messages. For news coverage, see www.nytimes.com/2005/02/05/technology/05spam.html and/or www.washingtonpost.com/wp-dyn/articles/A860-2004Jun23.html.

[59] I.B.M.'s DB2 Anonymous Resolution information at: www-306.ibm.com/software/data/db2/eas/anonymous/ This concept and similar applications are discussed at some length in the April 2002 book *Translucent Databases* by Peter Wayner. (ISBN 0967584418). An excellent overview and discussion by Simson Garfinkel of hash functions is available at: www.techreview.com/articles/04/08/wo_garfinkel080404.asp.

[60] Independent Centre for Privacy Protection (ICPP), *Identity Management Systems (IMS): Identification and Comparison Study* (September 2003), available at: www.datenschutzzentrum.de/download/IMS/IMS-Study-final.pdf.

[61] Mogul, Richard, "Danger Within – Protecting your Company from Internal Security Attacks," *CSO Online*, August 21, 2002, http://www.csoonline.com/analyst/report400.html.

[62] Computer Security Institute/FBI Computer Crime and Security Survey, 2002.

[63] For details, see www.realuser.com, www.realuser.com/news/pdf/Pictures%20as%20passwords%20-%20Economist.pdf , http://csrc.nist.gov/pki/twg/y2003/papers/twg-03-11.pdf and www.mddailyrecord.com/guestbook/realuser.html.

[64] See www.equifax.com/EFX_Canada/services_and_solutions/ecommerce_solutions/eidsol_e.html.

[65] See Ann Cavoukian, Ph.D., Information and Privacy Commissioner/Ontario, Security Technologies Enabling Privacy (STEPs): Time for a Paradigm Shift (June 2002) available at: www.ipc.on.ca/docs/steps.pdf.

[66] Global Information Security Survey 2004, Ernst & Young, page 21.

[67] Cited in Ponemon, Larry, "Opinion: After a privacy breach, how should you break the news?" (July 5, 2005) in ComputerWorld at www.computerworld.com/securitytopics/security/privacy/story/0,10801,102964,00.html.

Select Bibliography

Relevant IPC Publications:

Identity Theft: Who's Using Your Name?
Ann Cavoukian, Ph.D., Information and Privacy Commissioner/Ontario, June 1997
Paper looks at what identity theft is, how it occurs, why people should be concerned, and what consumers and organizations can do to minimize their chances of being victimized. In particular, technological ways of protecting one's personal information are explored.
URL: www.ipc.on.ca/scripts/index_.asp?action=31&P_ID=11407&N_ID=1&PT_ID=11351&U_ID=0
PDF format: www.ipc.on.ca/docs/idtheft-e.pdf

Identity theft and your credit report: What you can do to protect yourself
Provides guidelines on what to do about your credit report if your identity/identification has been stolen.
Ann Cavoukian, Ph.D., Information and Privacy Commissioner/Ontario, June 1997, Revised Feb. 2003
URL: www.ipc.on.ca/scripts/index_.asp?action=31&P_ID=11307&N_ID=1&PT_ID=11301&U_ID=0
PDF format: www.ipc.on.ca/docs/credit.pdf

The Security-Privacy Paradox: Issues, Misconceptions and Strategies
Joint Report by Ann Cavoukian, Ph.D., Information and Privacy Commissioner/Ontario
and Deloitte & Touche, August 2003
This joint paper provides hands-on advice for developing strategies for information security and privacy protection.
URL: www.ipc.on.ca/scripts/index_.asp?action=31&P_ID=14447&N_ID=1&PT_ID=11351&U_ID=0
PDF format: www.ipc.on.ca/userfiles/page_attachments/sec-priv.pdf

What to do if a privacy breach occurs: Guidelines for government organizations
Ann Cavoukian, Ph.D., Information and Privacy Commissioner/Ontario, May 2003
This paper is aimed at government organizations but the guidelines can be used by all organizations.
URL: www.ipc.on.ca/scripts/index_.asp?action=31&P_ID=14323&N_ID=1&PT_ID=11351&U_ID=0
PDF format: www.ipc.on.ca/docs/prbreach.pdf

Security Technologies Enabling Privacy (STEPs): Time for a Paradigm Shift
Ann Cavoukian, Ph.D., Information and Privacy Commissioner/Ontario, June 2002
Many security technologies can be redesigned to minimize or eliminate their privacy invasive features, yet remain highly effective tools.
URL: www.ipc.on.ca/scripts/index_.asp?action=31&P_ID=13289&N_ID=1&PT_ID=11351&U_ID=0
PDF format: www.ipc.on.ca/docs/steps.pdf
7 Essential STEPs (PDF): www.ipc.on.ca/userfiles/page_attachments/7steps.pdf

Privacy and Boards of Directors: What You Don't Know Can Hurt You
Ann Cavoukian, Ph.D., Information and Privacy Commissioner/Ontario, November 2003
Paper raises awareness of privacy as a business issue, not just a compliance issue.
URL: www.ipc.on.ca/scripts/index_.asp?action=31&P_ID=14759&N_ID=1&PT_ID=11351&U_ID=0
PDF format: www.ipc.on.ca/docs/director.pdf

Privacy Diagnostic Tool (PDT) Workbook
The Privacy Diagnostic Tool (PDT) is a self-assessment program used to help businesses gauge their privacy readiness by comparing their information processes with international privacy principles. Developed by the IPC with the assistance of Guardent and PricewaterhouseCoopers.
URL: www.ipc.on.ca/scripts/index_.asp?action=31&P_ID=12081&N_ID=1&PT_ID=11&U_ID=0
PDF Workbook: www.ipc.on.ca/userfiles/page_attachments/pdt.pdf
FAQ: www.ipc.on.ca/scripts/index_.asp?action=31&P_ID=11455&N_ID=1&PT_ID=12081&U_ID=0

Promoting Transparency through the Electronic Dissemination of Information

Ann Cavoukian, Ph.D., Information and Privacy Commissioner/Ontario, April 2004
URL: www.ipc.on.ca/scripts/index_.asp?action=31&P_ID=15393&N_ID=1&PT_ID=11351&U_ID=0
PDF format: www.ipc.on.ca/docs/protrans.pdf

Moving Information: Privacy & Security Guidelines
Ann Cavoukian, Ph.D., Information and Privacy Commissioner/Ontario, July 1997
Provides tips to assist organizations to ensure that the privacy and security of personal and confidential information have been accounted for during all phases of a move, from retention and disposal of records to providing secure transportation and, finally, to establishing a secure location once they reach the final destination.
URL: www.ipc.on.ca/scripts/index_.asp?action=31&P_ID=11421&N_ID=1&PT_ID=11351&U_ID=0
PDF format: www.ipc.on.ca/userfiles/page_attachments/moving.pdf

Guidelines on Facsimile Transmission Security
Ann Cavoukian, Ph.D., Information and Privacy Commissioner/Ontario, Revised January 2003
Sets out guidelines for government organizations to consider when developing systems and procedures to maintain the confidentiality and integrity of information transmitted by fax.
URL: www.ipc.on.ca/scripts/index_.asp?action=31&P_ID=11403&N_ID=1&PT_ID=11351&U_ID=0
PDF format: www.ipc.on.ca/docs/fax-gd-e.pdf

Incorporating Privacy into Marketing and Customer Relationship Management
Joint Report of the Office of the Information and Privacy Commissioner/Ontario
and the Canadian Marketing Association, May 2004
URL: www.ipc.on.ca/scripts/index_.asp?action=31&P_ID=15173&N_ID=1&PT_ID=11351&U_ID=0
PDF format: www.ipc.on.ca/docs/priv-mkt.pdf

Data Mining: Staking a Claim on Your Privacy
Ann Cavoukian, Ph.D., Information and Privacy Commissioner/Ontario, January 1998
Discusses a growing practice that businesses are using to sharpen their competitive edge. Without safeguards, data mining can jeopardize informational privacy.
URL : www.ipc.on.ca/scripts/index_.asp?action=31&P_ID=11387&N_ID=1&PT_ID=11351&U_ID=0
PDF format: www.ipc.on.ca/docs/datamine.pdf

Cross-National Study of Canadian and U.S. Corporate Privacy Practices.
Joint Study by the Office of the Information and Privacy Commissioner/Ontario and the Ponemon Institute, May 2004.
This joint study benchmarks the corporate privacy practices of Canadian and U.S. companies.
URL: www.ipc.on.ca/scripts/index_.asp?action=31&P_ID=15525&N_ID=1&PT_ID=11351&U_ID=0
PDF format: www.ipc.on.ca/docs/cross.pdf

Index of Recent Speeches and Presentations:
URL: www.ipc.on.ca/scripts/index_.asp?action=31&P_ID=11527&N_ID=1&PT_ID=21&U_ID=0

External Sources Consulted

Ambeo, Ken Richardson, Data Piracy: The Threat From Within
The Data Administration Newsletter, January 2005
URL: www.tdan.com/i031hy04.htm

Anderson, Ross, Why Information Security is Hard - An Economic Perspective, 2001
URL: www.ftp.cl.cam.ac.uk/ftp/users/rja14/econ.pdf

Bishop, Toby J.F. & Warren, John, Identity Theft: The Next Corporate Liability Wave?
The Corporate Counsellor, March 30, 2005
URL: www.law.com/jsp/cc/pubarticleCC.jsp?id=1112090711870

Blundon, William, Building a Single View of Customers
May 02, 2005
URL: www.destinationcrm.com/articles/default.asp?ArticleID=5015

Cate, Fred. H.
"The Failure of Fair Information Practice Principles"
Forthcoming chapter in *Consumer Protection in the Age of the 'Information Economy'*

Chubb Insurance, One in Five Americans Has Been a Victim of Identity Fraud
News release, July 7, 2005
URL: www.chubb.com/corporate/chubb3875.html

Claburn, Thomas, Privacy Pays for Banks
InformationWeek, April 5, 2005
URL: www.informationweek.com/story/showArticle.jhtml?articleID=160500671
Ponemon/Watchfire Study: www.watchfire.com/resources/privacy-survey.pdf

CSI/FBI Computer Crime and Security Survey, various years
URL: www.gocsi.com/forms/fbi/csi_fbi_survey.jhtml

Cunningham , Darren & Elliott, Timo, The Burden of Trusted Information
DMReview, June 2005
URL: www.dmreview.com/editorial/dmreview/print_action.cfm?articleId=1028734

Federal Trade Commission,
—National and State Trends in Fraud & Identity Theft, Jan–Dec 2004, February 1, 2005
URL: www.consumer.gov/sentinel/pubs/Top10Fraud2004.pdf
—Identity Theft Survey Report (Synovate) September 2003
URL: www.ftc.gov/os/2003/09/synovatereport.pdf
—Workshop Report: Technologies for Protecting Personal Information, June 2003
URL: www.ftc.gov/bcp/workshops/technology/finalreport.pdf
Workshop Home: www.ftc.gov/bcp/workshops/technology/

Syverson, Paul, The Paradoxical Value of Privacy, March 14, 2003
URL: www.cpppe.umd.edu/rhsmith3/papers/Final_session3_syverson.pdf

EDS Canada, Privacy and Identity Management Survey
Summary of Results and Findings, 31 January 2005
URL: www.ipsos-na.com/news/pressrelease.cfm?id=2543
Paper: www.ipsos-na.com/news/client/act_dsp_pdf.cfm?name=mr050131-2A.pdf&id=2543

Ernst & Young,
Global Information Security Survey 2004
URL: www.ey.com/GLOBAL/content.nsf/International/Press_Release_-_2004_Global_Information_Security_Survey

European Commission Joint Research Centre, Identity Theft: A Discussion Paper, 2004
URL: www.prime-project.eu.org/public/prime_products/papers/studies/IDTheftFIN.pdf

Evans, Bob, Business Technology: If Data Is Breached, Do The Right Thing
InformationWeek, April 25, 2005
URL: www.informationweek.com/showArticle.jhtml?articleID=161501155

Garvey, Martin J., Vendors Partner on Data Encryption
InformationWeek, May 9, 2005
URL: www.informationweek.com/story/showArticle.jhtml?articleID=163100098

Government of Canada, Consumer Measures Committee,
Discussion Paper: Working Together to Prevent Identity Theft (July 2005)
URL: http://cmcweb.ca/epic/internet/incmc-cmc.nsf/en/fe00097e.html

Hamilton, Tyler, Web, databases feed identity theft
The Toronto Star, Dec. 9, 2002
URL: www.tecrime.com/llart116.htm

Hendricks, Evan, When Your Identity Is Their Commodity
Washington Post, Sunday, March 6, 2005
URL: www.washingtonpost.com/wp-dyn/articles/A9101-2005Mar5.html

Ingrian Networks, Data Privacy in the Enterprise: Best Practices or Implementation
URL: www.ingrian.com/resources/

Ipsos-Reid,
Concern About Identity Theft Growing in Canada
Eighty Percent of Canadians Think Identity Theft Is a Serious Problem; One-Third More Concerned Than a Year Ago, Ipsos-Reid, February 28, 2005
URL: www.ipsos-na.com/news/pressrelease.cfm?id=2582

Jericho Forum, Visioning White Paper, February 2005
URL: www.opengroup.org/jericho/doc.tpl?CALLER=index.tpl&gdid=6809
URL: www.opengroup.org/projects/jericho/uploads/40/6809/vision_wp.pdf

Kelly, C.J., The Cost of Securing the People's Privacy
Security Manager's Journal, May 02, 2005
URL: www.computerworld.com/securitytopics/security/story/0,10801,101408,00.html

Lawson, Philippa and Lawford, John, Identity Theft: The Need for Better Consumer Protection"
Public Interest Advocacy Centre, November 5, 2003
URL: www.piac.ca/ID_Press_Release.pdf

Martin, Steven, Banks Make Permanent Free ID-Theft Assistance
InformationWeek, April 13, 2005
URL: www.informationweek.com/story/showArticle.jhtml?articleID=160702119

McAlearney, Shawna, Lawsuit could amplify data protection laws
SearchSecurity.com, February 28, 2005
URL: http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1062438,00.html

Nevins, Scott, Database Security – Protecting Sensitive and Critical Information
DMReview, January 2003
URL: www.dmreview.com/editorial/dmreview/print_action.cfm?articleId=6310

Office of the Alberta Information and Privacy Commissioner
Investigations find Alberta businesses failed to protect personal information from identity thieves
News release, February 8, 2005
URL: www.oipc.ab.ca/news/DetailsPage.cfm?ID=1780

Olsen, Florence, Shopping for data: Lawmakers have tough questions for largely unregulated data firms"
Federal Computer Weekly, April 25, 2005
URL: www.fcw.com/article88676

Patton, Susannah, Privacy Is Your Business
CIO Magazine, June 1, 2004
URL: www.cio.com/archive/060104/privacy.html

Ponemon, Larry, The seven deadly sins of identity management
Opinion piece in *Computerworld*, May 20, 2005
URL: www.computerworld.com/securitytopics/security/story/0,10801,101893,00.html

Privacy Rights Clearinghouse
—A Chronology of Data Breaches Reported Since the ChoicePoint Incident
URL: www.privacyrights.org/ar/ChronDataBreaches.htm
—Prevent Identity Theft with Responsible Information-Handling Practices in the Workplace (updated April 2005)
URL: www.privacyrights.org/ar/PreventITWorkplace.htm
—Fact Sheet 12, A Checklist of Responsible Information Handling Practices (rev. May 2002),
URL: www.privacyrights.org/fs/fs12-ih2.htm

Public Policy Forum Roundtable on Identity Theft and Identity Fraud
Ottawa, 26 June 2003
URL: www.ppforum.ca/ow/identity_theft_fraud.pdf

Scalet, Sarah, The Five Most Shocking Things About the ChoicePoint Debacle"
CSO Magazine Online, May 2005
URL: www.csoonline.com/read/050105/choicepoint.html

Schweitzer, Douglas, Twelve mistakes security managers make
ComputerWorld, September 30, 2004
URL: www.computerworld.com/securitytopics/security/story/0,10801,96236,00.html

Solove, Daniel J. and Hoofnagle, Chris Jay, A Model Regime of Privacy Protection (Version 2.0)" (April 5, 2005), GWU Law School Public Law Research Paper No. 132.
URL: http://ssrn.com/abstract=699701

Solove, Daniel J., Identity Theft, Privacy, and the Architecture of Vulnerability
Hastings Law Journal, Vol. 54, p. 1227, 2003
URL: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=416740 | http://ssrn.com/abstract=416740

Stampley, Dave, "Three Ways to Prepare for the IT Impact of New Privacy Laws"
InformationWeek, May 2, 2005
URL: www.informationweek.com/story/showArticle.jhtml?articleID=161600945

Sullivan, Patrick F., Governing Data Assets: Data Governance – An Information Assurance Framework
Synomos Inc. white paper, November 2004
URL: www.synomos.com/html/resource-center/files/DataGovernanceWhitePaper.pdf

Truste Data Security Guidelines for Protecting Consumer Privacy, V1.1, May 10, 2005
URL: www.truste.org/pdf/SecurityGuidelines.pdf
Press Release: www.truste.org/about/press_release/04_25_05.php

Information and Privacy Commissioner/Ontario

2 Bloor Street East
Suite 1400
Toronto, Ontario
M4W 1A8

416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Website: www.ipc.on.ca